U.S. Department of Energy
Environmental Management Consolidated Business Center (EMCBC)
Information Resource Management (IRM) Rules of Behavior

In compliance with the requirements of OMB Circular A-130 Appendix III, as required by law under the Clinger-Cohen Act, all users of the U.S. Department of Energy (DOE) information technology (IT) systems are required to be informed of the rules of behavior that govern appropriate use. These rules apply to any/all U.S. DOE IT systems used to access U.S. DOE data. Users will be held accountable for their actions on all U.S. DOE IT systems. If an employee violates the EMCBC IRM Rules of Behavior, the employee may be subject to disciplinary action at the discretion of the U.S. DOE/ Office of the Chief Information Office (OCIO), and/or his or her employer's management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation and the judgment of the appropriate authority. These Rules of Behavior pertain to both classified and unclassified environments.

To ensure compliance with requirements in this regard, these Rules of Behavior shall establish evidence of such compliance on an individual basis. You are required to read and agree to the following Rules of Behavior and concur with your signature.

1. I will not install, copy, or download software unless expressly authorized by EMCBC IRM.
2. I will not disable any security features or alter any information system(s) configuration(s).
3. Federal employees, contractors, and other government representatives are permitted limited use of government equipment and/or resources for personal needs when such use involves de minimis additional expense to the government, does not interfere with the mission or operations of EMCBC DOE activities, does not violate the Standards of Ethical Conduct for Employees of the Executive Branch, and is permissible under DOE Orders and applicable State and other Federal Laws and regulations.

   Examples of appropriate use are (reference DOE O 203.1 for a list of additional appropriate uses):
   - Communication with a volunteer charity organization
   - Checking a Thrift Savings Plan (TSP) or other investment
   - Sending an occasional fax to transmit a form of personal use

   Except as explicitly allowed according to the above appropriate use section, the following are considered inappropriate uses of U.S. DOE IT systems (reference DOE O 203.1 for a list of additional inappropriate uses):

   - Conducting private and/or personal business activities
   - Using resources for amusement/entertainment purposes or to organize non-U.S. DOE sanctioned social events including sending holiday cards
   - Gambling
   - Disseminating non-business related E-Mails (sending E-Mails to large distribution groups) including E-Mail chains
   - Viewing or transmitting any sexually explicit materials and/or materials related to illegal activities
   - Using government equipment and/or resources as staging grounds to gain unauthorized access to other information systems

4. I have no expectation of privacy on any U.S. DOE IT systems.
5. Use of U.S. DOE data is restricted to authorized users and I am responsible for any/all actions taken through the use of my user account and/or access credentials.
6. If I have been given access permissions to process classified data, I will not enter data of a higher classification level than appropriate for the level of the classified system(s). Under no circumstances will I enter classified data into an unclassified system, nor will I allow anyone else to do so. If I mistakenly receive or disseminate any classified data I will immediately notify my supervisor/EMCBC Federal Sponsor (the EMCBC Federal employee that verified your need to access the EMCBC IT system) and EMCBC IRM.
7. E-Mails generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of the U.S. DOE.
8. E-Mail shall not be used for sensitive data transmissions outside of the network unless Entrust encryption is employed.
9. Upon the discovery of a security related incident, I will immediately stop work, report the cyber security incident(s) to my supervisor/Federal Sponsor and EMCBC IRM. Reportable cyber security incidents generally meet one of the following criteria:
   - All attempts at unauthorized access, whether or not they are successful, even if unauthorized access is suspected but not yet proven
   - Instances of malicious code such as viruses, trojans, worms, malware, adware, spyware, ransomeware, etc.
   - Situations where a person who does not appear to be conducting legitimate business is acting in a manner that raises suspicion
   - Instances where a user is in violation of these Rules of Behavior, unless explicitly authorized by the Assistant Director, IRM (ADIRM) or designee
   - Actual or probable loss of media containing Personally Identifiable Information (PII), or the disclosure of PII to unapproved person(s)
10. Should I discover or be notified of the possibility that my workstation, mobile devices, or network files may have been contaminated due to inadvertent receipt of classified information, I will immediately cease operation and contact my supervisor/Federal Sponsor and EMCBC IRM. The EMCBC IRM will arrange for the clearing or sanitization of the devices or files as appropriate.
11. The following access credentials/password requirements are applicable:
    - Passwords shall be changed every 90 days or at the request of EMCBC IRM.
    - The last 24 passwords cannot be reused.
    - Passwords should not contain the user ID, any common dictionary word(s), employ common names, or include my own, close friends, or relatives' names, social security numbers, date(s) of birth, phone numbers, or any other information associated with the user of the password. Passwords should not contain any simple pattern(s) of letters or numbers.
    - Sharing of access credentials/passwords is prohibited unless explicitly authorized by the ADIRM or designee.
    - Storing of clear-text access credentials/passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information is prohibited. Stored access credentials/passwords must be encrypted and/or password protected.
12. Each employee (both Federal and contractor) using U.S. DOE IT systems is responsible for identifying Controlled Unclassified Information (CUI), which includes Personally Identifiable Information (PII), on their individual portable devices (i.e., laptops, tablets) or removable media (i.e., thumb/flash drives, CDs). The following CUI requirements are applicable:
    - If there is a critical business need to store CUI on portable devices or removable media and transport it outside a secure U.S. DOE facility or access CUI remotely (i.e., Virtual Private Network (VPN), remote access), the employee must submit detailed justification to and obtain

approval from EMCBC IRM. If approved by EMCBC IRM, the data must be encrypted in accordance with approved procedures and removed from the device within 90 days.

- CUI data is only authorized to be stored on approved government systems.
- If a device containing protected PII is lost or stolen, or there is reason to suspect that unauthorized individuals have gained access to protected PII, it must be reported within 45 minutes of discovery to your supervisor/Federal Sponsor and EMCBC IRM.

13. The use of publicly accessible social media is authorized as needed to receive relevant work-associated public information. Users are prohibited from updating any publicly accessible social media unless explicitly authorized to do so in writing by the ADIRM (i.e., Facebook, Twitter, Snapchat).
14. Users shall not use their personal E-Mail accounts to store, process, or transfer government information.
15. I further certify that I am not a Foreign National.

New users are required to complete Cyber Security Awareness Training within 30-days of account creation.

Failure to do so will result in account lock-out.

USER ACKNOWLEDGMENT OF EMCBC IRM RULES OF BEHAVIOR

INSTRUCTIONS:
Fill out form electronically, print, sign (electronic signatures not accepted), and submit to IRM.

____
User Name

____ ______________________
User Signature Date

My above signature indicates that I acknowledge and will comply with the Environmental Management Consolidated Business Center (EMCBC) Office of Information Resource Management (IRM) Rules of Behavior.